JOURNAL OF ALGEBRA **207,** 511–524 (1998)
ARTICLE NO. JA987492

Generators of Central Simple Algebras

Zinovy Reichstein*

Department of Mathematics, Oregon State University, Corvallis, Oregon 97331
E-mail: zinovy@math.orst.edu

Received July 3, 1997

Let A be a finite-dimensional central simple algebra and let k be a subfield of its center $Z(A)$. We say that $z_1, \dots, z_m$ generate A as a central simple algebra over k if $A = S^{-1}k[z_1, \dots, z_m]$, where $S = k[z_1, \dots, z_m] \cap Z(A)^*$. In this paper we give a necessary and sufficient condition for A to be generated by m elements as a central simple algebra over k. © 1998 Academic Press

1. INTRODUCTION

Let A be a central simple algebra with center K and let k be a subfield of K. Given $z_1, \dots, z_m \in A$, we define the subalgebra $k(z_1, \dots, z_m) \subset A$ as the central localization $S^{-1}k[z_1, \dots, z_m]$, where $S = k[z_1, \dots, z_m] \cap K^*$. In other words, $k(z_1, \dots, z_m) = k(S)[z_1, \dots, z_m]$. In this paper we shall address the following question: Which finite-dimensional central simple algebras can be generated by m elements, i.e., are of the form $k(z_1, \dots, z_m)$? Note that if A is a finite-dimensional division algebra then $A = k(z_1, \dots, z_m)$ if and only if A is generated by $z_1, \dots, z_m$ as a division algebra over k; see Remark 3.2.

A partial answer to our question is given by the following theorem of Procesi.

THEOREM 1.1 (Procesi). *Let A be a central simple algebra of degree n, K be the center of A, and $k \subset K$. Suppose $A = k(z_1, \dots, z_m)$ for some $z_1, \dots, z_m \in A$. Then K is a finitely generated extension of k and* $\operatorname{trdeg}_k(K) \leq (m-1)n^2 + 1$. *Moreover, equality holds if and only if A is isomorphic (as a k-algebra) to the universal division algebra* $\mathrm{UD}(m, n)$.

* Partially supported by NSA Grant MDA904-9610022.

0021-8693/98 $25.00

A proof can be found in [P_2, Chap. 8, Sect. 3]; see also Lemma 4.1. Note that if we set $n = 1$ then $A = K$ and $\mathrm{UD}(m, n)$ is the purely transcendental field extension of k generated by m independent indeterminates. Thus in this case Theorem 1.1 reduces to familiar statements about fields, namely (i) a field extension K/k generated by m elements has transcendence degree $\leq m$ and (ii) equality holds if and only if K/k is purely transcendental.

Our main result is the following converse to Theorem 1.1.

THEOREM 1.2. *Let $m \geq 2$ and $n \geq 1$ be integers and A be a central simple algebra of degree n with center K. Suppose $k \subset K$ is a finitely generated separable field extension such that*

$$\mathrm{trdeg}_k(K) \leq (m-1)n^2.$$

Then $A = k(z_1, \ldots, z_m)$ for some $z_1, \ldots, z_m \in A$.

Note that in the case $n = 1$ (and thus $A = K$) Theorem 1.2 says that a finitely generated separable field extension K/k of transcendence degree $\leq m - 1$ is necessarily generated by m elements. The latter statement is a form of the primitive element theorem. Another interesting special case arises if we set $\mathrm{trdeg}_k(K) \leq 4$. In this case Theorem 1.2 says that if A is non-commutative, it can always be generated by 2 elements over k.

We give two proofs of Theorem 1.2. The argument presented in Section 5 is shorter and more direct; however, it only goes through if $\mathrm{char}(k) = 0$. A characteristic-free proof of Theorem 1.2 is given in Section 8; it relies on a general position argument with respect to the differential Zariski topology on $A^m \simeq K^{mn^2}$. This approach also yields additional information about the set of m-tuples of generators; see Remark 8.1.

2. PRELIMINARIES

The following notational convention will be used throughout the paper.

$Z(R)$	center of a ring R
m	integer ≥ 2
n	integer ≥ 1
k	base field
$k \subset K$	field extension
r	transcendence degree of K/k
A	central simple algebra of degree n with center K

$A(t)$	$= A \otimes_K K(t)$
$k[z_1, \ldots, z_m]$	k-subalgebra generated by $z_1, \ldots, z_m$
$k(z_1, \ldots, z_m)$	the algebra defined in the beginning of Section 1
$X_1, \ldots, X_m$	m generic $n \times n$-matrices
$\mathrm{UD}(m, n)$	$= k(X_1, \ldots, X_m)$, universal division algebra
$Z(m, n)$	center of $\mathrm{UD}(m, n)$
$d = (m - 1)n^2 + 1$	transcendence degree of $Z(m, n)/k$

We begin with a simple lemma which will be used in the sequel. Let e_{ij} be the elementary $n \times n$-matrix which has 1 in position (i, j) and 0 in every other position.

LEMMA 2.1. *Let $a = e_{11}$ and $b = e_{12} + \cdots + e_{n-1,n} + e_{n1} \in M_n$. Then every elementary $n \times n$-matrix e_{ij} can be expressed as a monomial in a and b.*

Proof. A simple induction argument shows that $b^s a = e_{n+1-s,1}$ and $ab^{t-1} = e_{1t}$ for every $s, t = 1, \ldots, n$. Thus

$$e_{ij} = e_{i1}e_{1j} = (b^{n+1-i}a)(ab^{j-1})$$

is a monomial in a and b. ∎

3. THE STRUCTURE OF $k(z_1, \ldots, z_m)$

Let A be a finite-dimensional central simple algebra with center K, let k be a subfield of K, and let $z_1, \ldots, z_m \in A$. In this section we take a closer look at the structure of the subalgebra $k(z_1, \ldots, z_m)$ defined in the beginning of Section 1. The next two lemmas describe it in the case where $z_1, \ldots, z_m$ generate A as a K-algebra. Note that this condition holds for $z_1, \ldots, z_m \in A$ in general position with respect to the Zariski topology on $A^m \simeq K^{mn^2}$; see Lemmas 7.1(b) and 7.2(b).

LEMMA 3.1. *Let A be a central simple algebra of degree n, $k \subset K = Z(A)$, and $z_1, \ldots, z_m \in A$. Then the following condition are equivalent*:

(a) $K[z_1, \ldots, z_m] = A$.

(b) $k(z_1, \ldots, z_m)$ *is a central simple algebra of degree* n.

Proof. Let $R = k[z_1, \ldots, z_m]$ and $B = k(z_1, \ldots, z_m)$.

Assume (a) holds. Since $KB = A$, R is a prime ring of PI degree n and $Z(R) \subset K$. Therefore,

$$S = R \cap K^* = Z(R) \setminus \{0\},$$

and $B = S^{-1}R$ is a central simple algebra of degree n by [Ro, Corollary 6.1.29].

To prove the opposite implication, note that $K[z_1, \dots, z_m] = KR = KB$ by the definition of B. If B is a central simple algebra of degree n then by the double centralizer theorem $KB = A$, and part (b) follows.

Remark 3.2. Given $z_1, \dots, z_m \in A$, let $k\langle\langle z_1, \dots, z_m \rangle\rangle$ be the smallest k-subalgebra R of A with the following properties: (i) $z_1, \dots, z_m \in R$ and (ii) $x^{-1} \in R$ whenever $x \in R$ and x is invertible in A. Clearly $k(z_1, \dots, z_m) \subset k\langle\langle z_1, \dots, z_m \rangle\rangle$; moreover, if A is a finite-dimensional central simple algebra and $K[z_1, \dots, z_m] = A$ then equality holds by Lemma 3.1. In particular, $k(z_1, \dots, z_m) = A$ if and only if $k\langle\langle z_1, \dots, z_m \rangle\rangle = A$. Thus Theorems 1.1 and 1.2 remain true if one replaces $k(z_1, \dots, z_m)$ by $k\langle\langle z_1, \dots, z_m \rangle\rangle$. We chose to work with $k(z_1, \dots, z_m)$ because it allowed us to state Theorem 1.1 in the form it was originally proved by Procesi in [P_2]. On the other hand, if one were to investigate how many elements are required to generate an infinite-dimensional division algebra, it would be natural to define the algebra generated by $z_1, \dots, z_m$ as $k\langle\langle z_1, \dots, z_m \rangle\rangle$.

LEMMA 3.3. *Let A be a central simple algebra of degree n, $k \subset K = Z(A)$, and $z_1, \dots, z_m \in A$ such that $A = K[z_1, \dots, z_m]$. Let $K_0 = k(\operatorname{tr} P(z))$, as $P(z)$ ranges over all monomials in $z = (z_1, \dots, z_m)$ and let $\Lambda = K_0[z_1, \dots, z_m]$. Then*

(a) $Z(\Lambda) = K_0$, *and*

(b) $\Lambda = k(z_1, \dots, z_m)$.

Proof. (a) Let c be a central element of Λ. Since $K[z_1, \dots, z_m] = A$, there is a monomial $P(z)$ in $z_1, \dots, z_m$ such that $\operatorname{tr} P(z) \neq 0$. (Note that if $\operatorname{char}(k)$ does not divide n, we can simply take $P(z) = 1$.) Writing c as $\operatorname{tr}(cP(z))/\operatorname{tr}(P(z))$ and remembering that $c \in \Lambda = K_0[z_1, \dots, z_m]$, we conclude that $c \in K_0$.

(b) By Lemma 3.1, $k(z_1, \dots, z_m)$ is a central simple algebra of degree n. Hence, it is closed under the (reduced) trace function $A \to K$. Consequently, $K_0 \subset k(z_1, \dots, z_m)$ and thus $\Lambda \subset k(z_1, \dots, z_m)$. On the other hand, since the center of Λ is a field by part (a), we have $k(z_1, \dots, z_m) \subset K_0(z_1, \dots, z_m) = \Lambda$. Thus $k(z_1, \dots, z_m) = \Lambda$, as claimed. ∎

Let $x_{ab}^{(i)}$ be mn^2 independent commuting indeterminates over k; here $a, b = 1, \dots, n$ and $i = 1, \dots, m$. Suppose $A = M_n(K)$, where $K = k(x_{ab}^{(i)})$ and

$$X_1 = \left(x_{ab}^{(1)}\right), \dots, X_m = \left(x_{ab}^{(m)}\right) \in A$$

are m generic $n \times n$-matrices. The algebra $k(X_1, \dots, X_m)$ is called the universal division algebra $\mathrm{UD}(m, n, k)$ (or $\mathrm{UD}(m, n)$ for short). This algebra was first introduced by Procesi who proved that it is, in fact, a division algebra and that its center $Z(m, n)$ has transcendence degree $(m-1)n^2 + 1$ over k; see [P_1, Part II]. The structure of $\mathrm{UD}(m, n)$ has since been extensively studied, see, e.g., [Ro, 7.1].

Remark 3.4. Lemma 3.3 shows that $Z(m, n) = k(\mathrm{tr}\, P(X))$, where $P(X)$ ranges over all monomials in the generic matrices $X_1, \dots, X_m$. (This fact is proved directly in [P_1, II.1.3].) Thus $Z(m, n) = \mathrm{Frac}(S)$, where $S = k[\mathrm{tr}\, P(X)]$.

Let A be a central simple algebra of degree n. Since the reduced trace is well-defined on A, we can evaluate $s(z)$ for any $s \in S$ and any $z = (z_1, \dots, z_m) \in A$. Moreover, if $s(z) = 0$ for every $z \in A^m$ then $s = 0$ in $Z(m, n)$. Indeed, otherwise s would give rise to an identity which holds in A but is not satisfied by the generic matrices, contradicting [Ro, 6.1.46′].

Now suppose $s \in Z(m, n)$ and $z = (z_1, \dots, z_m) \in A^m$. We shall say that $s(z)$ is defined if s can be written as a/b with $a, b \in S$, and $b(z) \neq 0$. In this case we set $s(z) = a(z)/b(z)$; this element of K depends only s and z, not on the choice of a and b. Note that every $s \in Z(m, n)$ is defined on a dense Zariski open subset of A^m (viewed as an mn^2-dimensional $Z(A)$-vector space.)

4. A REDUCTION LEMMA

LEMMA 4.1. *Let A be a finite-dimensional central simple algebra with center K. Suppose k is a subfield of K and $A = k(z_1, \dots, z_m)$ for some $z_1, \dots, z_m \in A$. Then K is a finitely generated field extension of k.*

Proof. Denote the degree of A by n. Then $A \subset M_n(L)$, where L is a splitting field of A. Write z_i as a matrix $(l_{ab}^{(i)}) \in M_n(L)$. Then $K \subset k(l_{ab}^{(i)})$, where $i = 1, \dots, m$ and $a, b = 1, \dots, n$. Thus K is finitely generated over k. ∎

LEMMA 4.2. *Let A be a central simple algebra of degree n, K be the center of A, and $A(t) = A \otimes_K K(t)$, where t is an independent central indeterminate. Assume that K is an infinite field, k is a subfield of K, and $A(t) = k(t)(z_1, \dots, z_m)$ for some $z_1, \dots, z_m \in A(t)$. Then $A = k(\bar{z}_1, \dots, \bar{z}_m)$ for some $\bar{z}_1, \dots, \bar{z}_m \in A$.*

Proof. For $i = 1, \dots, m$ write $z_i = \alpha_i(t)\beta_i^{-1}(t)$, where $\alpha_i \in A[t]$ and $0 \neq \beta_i \in K[t]$. We want to specialize t to $c \in K$ so that the m-tuple $z = (z_1, \dots, z_m)$ will specialize to an m-tuple $\bar{z} = (\bar{z}_1, \dots, \bar{z}_m)$ of generators of A. In fact, we claim that any $c \in K$ will do, except for a finite number.

Indeed, for all but finitely many $c \in K$, $\beta_i(c) \neq 0$ and thus $\bar{z}_i = \alpha_i(c)\beta_i^{-1}(c)$ is well defined for every $i = 1, \dots, m$. Moreover, we claim that

(a) for all but finitely many $c \in K$, we have $K[\bar{z}_1, \dots, \bar{z}_m] = A$ and

(b) for all but finitely many $c \in K$, the center of $k(\bar{z}_1, \dots, \bar{z}_n)$ equals K.

Note that if both (a) and (b) are satisfied then clearly $k(\bar{z}_1, \dots, \bar{z}_n) = A$. It therefore remains to prove (a) and (b). To prove (a), choose a K-basis $b_1, \dots, b_{n^2}$ of A. Note that these elements also form a $K(t)$-basis of $A(t)$. By Lemma 3.1, $K(t)[z_1, \dots, z_m] = A(t)$. This means that there are n^2 monomials $P_1(z), \dots, P_{n^2}(z)$ in $z_1, \dots, z_m$ which form a $K(t)$-basis of $A(t)$. Write $P_i(z) = \sum_j a_{ij}(t)b_j$, where $a_{ij}(t) \in K(t)$. Then the (base change) matrix $(a_{ij}(t))$ will be non-singular. This means that for all but finitely many $c \in K$, the matrix $(a_{ij}(c))$ is well-defined and non-singular. This, in turn, implies (a), as claimed.

In order to prove (b), recall that by Lemma 4.1, $K(t)$ is a finitely generated field extension of $k(t)$. Hence, $K(t)$ is finitely generated over k and, consequently, K is finitely generated over k. Write $K = k(y_1, \dots, y_r)$. By Lemma 3.3, $K(t)$ is generated over $k(t)$ by elements of the form $\mathrm{tr}(P(z))$, where $P(z)$ ranges over all monomials in $z_1, \dots, z_m$. Thus we can write

$$y_i = \frac{g_i\big(\mathrm{tr}(P_1(z)), \dots, \mathrm{tr}(P_s(z))\big)}{h_i\big(\mathrm{tr}(P_1(z)), \dots, \mathrm{tr}(P_s(z))\big)}, \tag{1}$$

where $P_1, \dots, P_s$ is a finite collection of monomials and $g_1, h_1, \dots, g_s, h_s$ are (commutative) polynomials in s variables over $k(t)$. In fact, after multiplying through by a common denominator, we may assume that every coefficient of every g_i and every h_i lies in $k[t]$. Note that the left hand side of (1) is independent of t and that the numerator and the denominator of the right hand side are both elements of $K(t)$. Thus if we specialize t to $c \in K$ (i) away from the poles of the numerator, (ii) away from the zeros and the poles of the denominator, and (iii) so that each $\bar{z}_i = z_i(c)$ is well-defined then

$$y_i = \frac{g_i\big(\mathrm{tr}(P_1(\bar{z})), \dots, \mathrm{tr}(P_s(\bar{z}))\big)}{h_i\big(\mathrm{tr}(P_1(\bar{z})), \dots, \mathrm{tr}(P_s(\bar{z}))\big)}.$$

Note that condition (i), (ii), and (iii) above only exclude a finite number of $c \in K$. If we now choose $c \in K$ so that condition (a) is satisfied, in addition to (i), (ii), and (iii), then by Lemma 3.3 each y_i will lie in the

center of $k(\bar{z}_1, \ldots, \bar{z}_m)$. By our choice of $y_1, \ldots, y_s$ this implies that the center of $k(\bar{z}_1, \ldots, \bar{z}_m)$ equals K, as claimed. This concludes the proof of (b) and thus of Lemma 4.2. ∎

5. PROOF OF THEOREM 1.2 IN CHARACTERISTIC ZERO

LEMMA 5.1. *Assume* $\mathrm{char}(k)$ *does not divide* n. *Let* $Y_1 = X_1 - n^{-1}\mathrm{tr}(X_1)$ *and let* $E = k(Y_1, X_2, \ldots, X_n) \subset \mathrm{UD}(m, n)$. *Then* $\mathrm{trdeg}_k Z(E) = (m-1)n^2$.

Proof. A central element of E commutes with $Y_1, X_2, \ldots, X_n$ and, hence, is central in $\mathrm{UD}(m, n)$. In other words, $Z(E) \subset Z(m, n)$; we claim $Z(E)(\mathrm{tr}(X_1)) = Z(m, n)$. Indeed, by Lemma 3.3 it is enough to show that $\mathrm{tr}(P(X_1, X_2, \ldots, X_m)) \in Z(E)(\mathrm{tr}(X_1))$ for every monomial P; the latter can be seen by substituting $X_1 = Y_1 + n^{-1}\mathrm{tr}(X_1)$ into $P(X_1, X_2, \ldots, X_n)$.

Therefore, $\mathrm{trdeg}_k Z(E) = (m-1)n^2$ or $(m-1)n^2 + 1$, depending on whether $\mathrm{tr}(X_1)$ is transcendental or algebraic over $Z(E)$. To rule out the second possibility, let $\phi\colon k[x_{ab}^{(i)}] \to k[x_{ab}^{(i)}]$ be the ring homomorphism which takes $x_{ij}^{(1)}$ to the (i, j)-entry of Y_1 and takes $x_{ab}^{(i)}$ to itself for every $i \geq 2$. Let $S = k[\mathrm{tr}\, P(X)]$ be as in Remark 3.4. Then ϕ restricts to a map $S \to S$. By Lemma 3.3, $Z(E)$ is the fraction field of $\phi(S)$. Since $\phi(\mathrm{tr}\, Y_1) = 0$, we have

$$\mathrm{trdeg}_k Z(E) = \mathrm{trdeg}_k \phi(S) < \mathrm{trdeg}_k S = \mathrm{trdeg}_k Z(m, n) = (m-1)n^2 + 1.$$

Thus $\mathrm{trdeg}_k Z(E) = (m-1)n^2$, as claimed. ∎

We are now ready to prove Theorem 1.2 under the assumption that $\mathrm{char}(k) = 0$. In view of Lemma 4.2 we may assume without loss of generality that

$$\mathrm{trdeg}_k(K) = (m-1)n^2.$$

Indeed, if $\mathrm{trdeg}_k(K) < (m-1)n^2$ then we can replace A by $A(t)$ and appeal to Lemma 4.2. Note that if $A(t) = k(z_1, \ldots, z_m)$ then certainly $A(t) = k(t)(z_1, \ldots, z_m)$.

Suppose $\mathrm{trdeg}_k(K) = (m-1)n^2$. Then by [RV, Theorem 1.1], $A(t)$ contains a copy of $\mathrm{UD}(m, n)$ and, in particular, a copy of $E = k(Y_1, X_2, \ldots, X_m)$. By Lemma 5.1,

$$\mathrm{trdeg}_k Z(E) = (m-1)n^2 = \mathrm{trdeg}_k(K). \tag{2}$$

Thus by [RV, Proposition 3.2] E embeds in A, i.e., we may assume $A = E \otimes_{Z(E)} K$, where K is a finite extension of $Z(E)$ by (2). By the primitive element theorem $K = Z(E)(\alpha)$ for some $\alpha \in K$. We now claim that $A = k(z_1, \dots, z_m)$, where $z_1 = Y_1 + n^{-1}\alpha$, $z_2 = X_2, \dots, z_m = X_m$. Note that since $K[z_1, \dots, z_n] = A$, $k(z_1, \dots, z_m)$ is a central simple subalgebra of A of degree n; see Lemma 3.1. In particular, $k(z_1, \dots, z_m)$ contains $\alpha = \mathrm{tr}(z_1)$ and thus $Y_1 = z_1 - n^{-1}\alpha$, as well as $X_2, \dots, X_m$. Since $k(z_1, \dots, z_m)$ contains both $E = k(Y_1, X_2, \dots, X_m)$ and $\alpha = \mathrm{tr}(X_1)$, it is equal to all of A, as claimed. ∎

Remark 5.2. We would now like to turn this argument into a characteristic-free proof of Theorem 1.2. With this in mind, note that we have used the assumption $\mathrm{char}(k) = 0$ in three instances: (i) E is only defined if n is invertible in k, (ii) the reduction to the case where $\mathrm{trdeg}_k(K) = (m-1)n^2$ requires the use of Lemma 4.2 which assumes that K is an infinite field, and (iii) the definition of α depends on the primitive element theorem which may fail in prime characteristic.

A closer examination shows that (i) and (ii) can be bypassed in prime characteristic. Indeed, (i) the definition of E can be adjusted by setting Y_1 to be $X_1/\mathrm{tr}(X_1)$ instead of $X_1 - n^{-1}\mathrm{tr}(X_1)$. If we then define $z_1 = \alpha Y_1$ rather than $Y_1 + n^{-1}\alpha$, the rest of the argument will go through unchanged. On the other hand, (ii) only presents a problem if K is finite. However, in this case the situation is greatly simplified by Wedderburn's theorem and can be handled separately; see Section 8.

The use of the primitive element theorem presents a more serious difficulty. In order to overcome it we will (a) assume that K is separable over k (note that without this assumption Theorem 1.2 fails even for $n = 1$) and (b) use the results of Section 7 instead of [RV, Theorem 1.1 and Proposition 3.2].

6. SEPARABLE EXTENSION

Let $k \subset K$ be a field extension. Recall that $t_1, \dots, t_r \in K$ are said to form a separating transcendence basis for a field extension $k \subset K$ if (i) they are algebraically independent over k and (ii) K is separable algebraic over $k(t_1, \dots, t_r)$. An extension $k \subset K$ is separable of transcendence degree r if it admits a separating transcendence basis $t_1, \dots, t_r$. In this case the k-derivations

$$D_i = \partial/\partial t_i \colon K \to K$$

are uniquely defined and form a basis of the K-vector space $\mathrm{Der}_k(K)$ of derivations from K to itself. For details see [L] or [C].

LEMMA 6.1. *Elements $s_1, \dots, s_r \in K$ form a separating transcendence basis of K/k iff the Jacobian matrix $J = (D_i(s_j)) = (\partial s_i / \partial t_j) \in M_n(K)$ is non-singular.*

Proof. The lemma follows from [L, X.7.10]. Indeed, the elements of the ith row of J are the coordinates of the Kähler differential ds_i in terms of the basis $dt_1, \dots, dt_r$ of $\mathrm{Der}_k(K)^*$. ∎

Recall that a field extension K/k is called unirational if K is contained in a purely transcendental extension of k.

LEMMA 6.2. *Every unirational field extension is separable.*

Proof. This follows from [L, X.5 and X.6]. ∎

Note that Lemma 6.2 implies, in particular, that the extension $k \subset Z(m, n)$ is separable. This fact will be repeatedly used in the sequel.

LEMMA 6.3. *Let $s_1, \dots, s_d$ be a separating transcendence basis of $Z(m, n)$ over k and let L be an infinite field containing k. Then there exists a dense Zariski open subset U of L^d with the following property. For every $(c_1, \dots, c_d) \in U$ there exist a finite separable field extension L'/L and an m-tuple of matrices $z = (z_1, \dots, z_m)$ such that $z_1, \dots, z_m \in M_n(L')$ and $s_i(z) = c_i$ for $i = 1, \dots, d$.*

The integer d in the statement of the lemma equals $(m-1)n^2 + 1 = \mathrm{trdeg}_k Z(m, n)$. We also note that $s_i(z) = c_i$ implies, in particular, that $s_i(z)$ is defined; see Remark 3.4.

Proof. Let K be a finite separable extension of $Z(m, n)$ which splits $\mathrm{UD}(m, n)$. Note that there are many such extensions (see [Ro, 7.1.2]); in particular, we can take $K = Z(m, n)(X_1)$ (see [P$_1$, II.1.7]).

We can now think of the generic matrices $X_1, \dots, X_m$ as elements of $M_n(K)$, say, $X_i = (y_{ab}^{(i)})$, where $y_{ab}^{(i)} \in K$ for each $a, b = 1, \dots, n$ and $i = 1, \dots, m$. Note that

$$s_i(X_1, \dots, X_m) = s_i; \tag{3}$$

see Remark 3.4.

Let $s = (s_1, \dots, s_d)$. Since K is finite and separable over $k(s)$, the Primitive Element Theorem says that $K = k(s)(\alpha)$, where α satisfies an irreducible polynomial $p(t) \in k(s)[t]$ with no repeated roots. In other words, the discriminant $\Delta(s)$ of this polynomial is a non-zero element of $k(s)$. Every element of K can now be written as a polynomial in α with coefficients in $k(s)$. In particular, we can write each $y_{ab}^{(i)}$ as $q_{ab}^{(i)}(\alpha)$ with $q_{ab}^{(i)}[t] \in k(s)[t]$.

Let $g = g(s_1, \dots, s_d) \in k[s]$ be a common denominator of the coefficients of $p(t)$ and $q_{ab}^{(i)}(t)$. In other words, we choose $g \neq 0$ so that $gp(t)$

and $gq_{ab}^{(i)}(t)$ lie in $k[s][t]$. Let U be the Zariski open dense subset of L^d consisting of d-tuples $c = (c_1, \dots, c_d)$ such that $g(c) \neq 0$ and $\Delta(c) \neq 0$. Given $c = (c_1, \dots, c_d) \in U$, we now proceed to construct the finite separable extension L'/L and the m-tuple of matrices $z_1, \dots, z_m \in M_n(L')$ such that $s_i(z_1, \dots, z_m) = c_i$.

We define L' as the splitting field of $\bar{p}(t)$, where $\bar{p}(t)$ is obtained by specializing each coefficient of $p(t)$. Since $g(c) \neq 0$, $\bar{p}(t)$ is indeed, well-defined. Moreover, since the discriminant $\bar{\Delta}(c)$ of $\bar{p}$ is non-zero, L' is a separable extension of L. Let $\bar{\alpha}$ be a root of $\bar{p}(t)$ in L'.

Finally, we define $z_1, \dots, z_m \in M_n(L')$ as follows. Let $R = k[s_1, \dots, s_d, 1/g(s)]$ and let $\mu\colon R[t] \to L'$ be given by $\mu(s_i) = c_i$ and $\mu(t) = \bar{\alpha}$. Since μ sends $p(t)$ to $\bar{p}(\bar{\alpha}) = 0$, it descends to a homomorphism $R[\alpha] \to L'$, which, in turn, gives rise to a homomorphism $\nu\colon M_n(R[\alpha]) \to M_n(L')$. Then each generic matrix $X_i = (q_{ab}^{(i)}(\alpha))$ lies in the domain of ν, and we define $z_i = \nu(X_i)$ for $i = 1, \dots, m$. Now (3) shows that $s_j(z_1, \dots, z_m) = \mu(s_j) = c_j$ for any $j = 1, \dots, d$, as claimed. ∎

7. THE DIFFERENTIAL ZARISKI TOPOLOGY

Let $k \subset K$ be a finitely generated separable extension. In this setting we can define the differential Zariski topology on K^N. A closed set in this topology is the zero locus of a collection of differential polynomials. Recall that a differential polynomial is a polynomial in x_i and $D_j(x_i)$, where $(x_1, \dots, x_n) \in K^N$ and $D_1, \dots, D_r$ is a basis of $\mathrm{Der}_k(K)$. For details we refer the reader to [RV, Sect. 4].

Suppose A is a central simple algebra of degree n. Denote the center of A by K. Then for any $m \geq 1$ we can view A^m as an mn^2-dimensional K-vector space. Explicitly, if $f_1, \dots, f_{n^2}$ is a K-basis of A then we identify $z = (z_1, \dots, z_m) \in A^m$ with $(\alpha_{ij}) \in K^{mn^2}$, where for $i = 1, \dots, m$

$$z_i = \sum_{j=1}^{n^2} \alpha_{ij} f_j. \tag{4}$$

If K/k is separable and $\mathrm{trdeg}_k(K) = r < \infty$ then $A^m \cong K^{mn^2}$ is endowed with the differential Zariski topology. Choose a collection of elements $s_1, \dots, s_r \in Z(m, n)$. We shall be interested in the following subsets of A^m,

$$\begin{aligned} V_1 &= \{(z_1, \dots, z_m) \in A^m \mid \mathrm{tr}(z_1) \neq 0\}, \\ V_2 &= \{(z_1, \dots, z_m) \in A^m \mid K[z_1, \dots, z_m] = A\}, \\ V_3 &= \{z \in A^m \mid s_1(z), \dots, s_r(z) \text{ form a separating transc. basis for } K/k\}. \end{aligned} \tag{5}$$

Note that if $z \in V_3$ then our definition presupposes that $s_1(z), \dots, s_r(z)$ are well defined; see Remark 3.4.

LEMMA 7.1. (a) *V_1 is Zariski open in A^m.*

(b) *V_2 is Zariski open in A^m.*

(c) *V_3 is open in the differential Zariski topology on A^m.*

Proof. (a) Let $z_1, \dots, z_m$ be as in (5). Then $\operatorname{tr}(z_1) = 0$ translates into a linear equation in α_{ij}.

(b) Observe that $K[z_1, \dots, z_m] = A$ if and only if the monomials $P(z)$ in $z_1, \dots, z_m$ span A as a K-vector space. Let $z_1, \dots, z_m$, be as in (4). Then $P(z) = \sum_{j=1}^{n^2} \beta_{Pj} f_j$, where each β_{Pj} is a polynomial in α_{ij}. Thus $K[z_1, \dots, z_m] \neq A$ if and only if every n^2 rows of the (infinite) $\times\, n^2$-matrix (β_{Pj}) are linearly dependent. The latter condition is equivalent to setting every $n^2 \times n^2$-minor of this matrix equal to 0. Thus the complement of V_2 in A^m is cut out by polynomial equations in α_{ij}.

(c) Let $S = k[\operatorname{tr} P(X)]$, where $P(X)$ ranges over all monomials in the generic matrices, as in Remark 3.4. Write $s_i = a_i/b_i$, where a_i and $b_i \in S$. Let $t_1, \dots, t_r$ be a separating transcendence basis for K/k and let $D_j = \partial/\partial t_j$ for $j = 1, \dots, r$. By Lemma 6.1 the elements $s_1(z), \dots, s_r(z)$ form a separating transcendence basis for K/k if and only if $\det(D_i(s_j)) \neq 0$. Suppose

$$b_j(z) \neq 0 \tag{6}$$

for every $j = 1, \dots, r$. Then $z \in V_3$ if and only if

$$\det\big(D_i(a_j)b_j - D_i(b_j)a_i\big)(z) \neq 0. \tag{7}$$

The inequalities (6) and (7) define a Zariski open set in the differential Zariski topology. This set depends on the choice of a_i and $b_i \in S$ such that $s_i = a_i/b_i$. Part (c) now follows from the fact that V_3 is the union of these open sets taken over all possible choices of $a_1, b_1, \dots, a_r, b_r$. ∎

LEMMA 7.2. (a) $V_1 \neq \emptyset$.

(b) *Assume $m \geq 2$. Then $V_2 \neq \emptyset$.*

(c) *Suppose k is an infinite field,* $\operatorname{trdeg}_k(K) = r \leq d = (m-1)n^2 + 1$, *and the set $s_1, \dots, s_r$ can be completed to a separating transcendence basis $s_1, \dots, s_d$ of $Z(m, n)$ over k. Then $V_3 \neq \emptyset$.*

Proof. Part (a) follows from the fact that $\operatorname{tr}(z_1)$ is a non-zero linear form of $A^m \cong K^{mn^2}$. To show that V_2 and V_3 are non-empty, it is enough to prove that $V_2(L) \neq \emptyset$ and $V_3(L') \neq \emptyset$ for some separable extension L and L' of K; see [RV, Theorem 4.3]. Choose a separable extension L/K which splits A; see [Ro, 7.1.12].

An element of $V_2(L)$ is thus an m-tuple of $n \times n$-matrices $z = (z_1, \dots, z_m) \in M_n(L)$ such that $L(z_1, \dots, z_m) = M_n(L)$. To show that $V_2(L) \neq \emptyset$, set

$$z_1 = e_{11}, \qquad z_2 = e_{12} + e_{23} + \cdots + e_{n-1,n} + e_{n1}, \qquad z_3 = 0, \dots, z_m = 0.$$

Then by Lemma 2.1, $(z_1, \dots, z_m) \in V_2(L)$. This proves part (b). (Other proofs of part (b) can be found in [P_2, III.1.2] or [Re, Lemma 2.10].)

To show that $V_3 \neq \emptyset$, we appeal to Lemma 6.3. Let $U \subset L^d$ be the Zariski open subset of Lemma 6.3 and let $U_1 \subset L^d$ be the set of all d-tuples $(c_1, \dots, c_d) \in L^d$ such that $c_1, \dots, c_r$ form a separating transcendence basis for L over k. By Lemma 6.1, U_1 is open in the differential Zariski topology on L^d. Since L^d is irreducible in the differential Zariski topology, we have $U \cap U_1 \neq \emptyset$; see [RV, Theorem 4.3]. Choose $(c_1, \dots, c_d) \in U \cap U_1$. Then by our choice of U there exists a finite separable extension L^1/L and $z_1, \dots, z_m \in M_n(L')$ such that $s_i(z_1, \dots, z_m) = c_i$ for $i = 1, \dots, d$. Since $(c_1, \dots, c_d) \in U_1$, we have $(z_1, \dots, z_m) \in V_3(L')$. This shows that $V_3(L') \neq \emptyset$ thus completing the proof of part (c). ∎

8. A CHARACTERISTIC-FREE PROOF OF THEOREM 1.2

First consider the case where K is finite. By Wedderburn's theorem $A = M_n(K)$; see [Ro, 7.1.11]. It is sufficient to show that $A = k(z_1, z_2)$ for some $z_1, z_2 \in A$. Choose a primitive element $\alpha \in K$ such that $k(\alpha) = K$ and define $z_1 = \alpha e_{11}$ and $z_2 = e_{12} + e_{23} + \cdots + e_{n1}$. We claim that $A = k(z_1, z_2)$. Indeed, $K[z_1, z_2] = K[e_{11}, z_2] = M_n(K)$ by Lemma 2.1. Thus by Lemma 3.3, $B = k(z_1, z_2)$ contains $\alpha = \mathrm{tr}(z_1)$. Consequently, $e_{11} = \alpha^{-1} z_1 \in B$ and thus $k[e_{11}, z_2] \subset B$. By Lemma 2.1, $k[e_{11}, z_2] = M_n(k)$. Since B contains both α and $M_n(k)$, we conclude that $B = A$, as claimed.

Now assume that K is infinite. By Lemma 4.2 we can replace A, K, and k by $A(t)$, $K(t)$, and $k(t)$. Note that $\mathrm{trdeg}_{k(t)} K(t) = \mathrm{trdeg}_k K$. The advantage of this setting is that the new base field $k(t)$ is always infinite. Thus we may assume without loss of generality that k is an infinite field.

Our argument will use a particular separating transcendence basis $s_1, \dots, s_d$ of $Z(m, n)$ over k which we now construct. Let $k_1 = k(\mathrm{tr}(X_1))$ and let $X_i = (x_{ab}^{(i)})$. Since

$$k_1 \subset Z(m, n) \subset k\left(x_{ab}^{(i)}\right)$$

and $k(x_{ab}^{(i)})$ is a purely transcendental extension of k_1, we conclude that $Z(m, n)$ is unirational over k_1 and thus, by Lemma 6.2, $Z(m, n)$ is separable over k_1. Recall that $Z(m, n) = k(\mathrm{tr}\, P(X))$, where $P(X)$ ranges

over the set of all monomials in $X_1, \dots, X_m$; see Lemma 3.3. Consequently, $Z(m, n) = k_1(\operatorname{tr} P(X))$. By [L, Proposition X.6.5] we can select a separating transcendence basis for the field extension $k_1 \subset Z(m, n)$ from the generating set $\{\operatorname{tr} P(X)\}$; denote the elements of this basis by $\operatorname{tr} P_1(X), \dots, \operatorname{tr} P_{d-1}(X)$. Suppose P_j is a monomial of degree e_j in X_1. Let $s_j = (\operatorname{tr} P_j(X))\operatorname{tr}(X_1)^{-e_j}$ for $j = 1, \dots, d-1$. Note that $k_1(s_1, \dots, s_{d-1}) = k_1(\operatorname{tr} P_1(X), \dots, \operatorname{tr} P_{d-1}(X))$ so that $s_1, \dots, s_{d-1}$ form a separating transcendence basis for $Z(m, n)$ over $k_1 = k(\operatorname{tr}(X_1))$. By our construction $s_i(z)$ is well-defined for any $z \in V_1$; see (5). Moreover,

$$s_i(\alpha z_1, z_2, \dots, z_m) = s_i(z_1, \dots, z_m) \tag{8}$$

for every $i = 1, \dots, d-1$ and every $0 \neq \alpha \in K$. Now set $s_d = \operatorname{tr}(X_1)$. Since s_d is transcendental over k, the elements $s_1, \dots, s_d$ form a separating transcendence basis for $Z(m, n)$ over k.

We are now ready to finish the proof of Theorem 1.2. Let V_1, V_2, and V_3 be as in (5). Since A^m is irreducible in the differential Zariski topology (see [RV, Theorem 4.3]) and V_1, V_2, and V_3 are non-empty open subsets of A^m (see Lemmas 7.1 and 7.2), we have $V_1 \cap V_2 \cap V_3 \neq \varnothing$. (Here we use the assumption that k is infinite.) Let $z = (z_1, \dots, z_m) \in V_1 \cap V_2 \cap V_3$, $A_0 = k(z_1, \dots, z_m)$, and

$$K' = k\big(s_1(z), \dots, s_r(z)\big). \tag{9}$$

Since $(z_1, \dots, z_m) \in V_2$, Lemma 3.1 says that A_0 is a central simple algebra of degree n and, in particular, $k(s_1(z), \dots, s_r(z)) \subset Z(A_0) \subset K$. Since $z \in V_3$, K is algebraic (and thus finite) and separable over K'. By the primitive element theorem $K = K'(\alpha)$ for some $0 \neq \alpha \in K$. We claim that

$$A = k(z_1', z_2, \dots, z_m), \tag{10}$$

where $z_1' = [\alpha/\operatorname{tr}(z_1)]z_1$. Indeed, since $(z_1, \dots, z_m) \in V_2$, we have

$$K[z_1', z_2, \dots, z_m] = K[z_1, \dots, z_m] = A. \tag{11}$$

Hence, by Lemma 3.1, $k(z_1', z_2, \dots, z_m)$ is a central simple algebra of degree n. In particular, it contains $s_i(z_1', z_2, \dots, z_m)$ for every $i = 1, \dots, d-1$. On the other hand, (8) says that $s_i(z_1, \dots, z_m) = s_i(z_1', z_2, \dots, z_m)$ for every $i = 1, \dots, d-1$. Since we are assuming $r \leq (m-1)n^2 = d-1$ this implies that $k(z_1', z_2, \dots, z_m)$ contains $K' = k(s_1(z), \dots, s_r(z))$. Moreover, it also contains $\alpha = \operatorname{tr}(z_1')$ and thus $K'(\alpha) = K$. We conclude that $k(z_1', z_2, \dots, z_m)$ contains $K[z_1', z_2, \dots, z_m]$, which is equal to all of A by (11). This completes the proof of (10) and thus of Theorem 1.2. ∎

Remark 8.1. If k is an infinite field, the above argument yields a more precise description of the set of m-tuples of generators of A under the assumptions of Theorem 1.2.

There exists a subset U of A^m such that (i) *U is open and dense in the differential Zariski topology and* (ii) *for any $z = (z_1, \dots, z_m) \in U$, we have $A = k(\beta z_1, z_2, \dots, z_m)$ for some $\beta \in K$.*

Here $U = V_1 \cap V_2 \cap V_3$; see (5). Given $z = (z_1, \dots, z_m) \in U$ let K' be as in (9). Then we can take $\beta = \alpha/\mathrm{tr}(z_1) \in K$, where α is any non-zero primitive element for the finite separable field extension $K' \subset K$. Note that primitive elements for this extension form a dense Zariski-open subset of K, viewed as a finite-dimensional K'-vector space. In this sense, a generically chosen element α (and thus β) of K will have the desired property.

ACKNOWLEDGMENTS

The question of which division algebras of transcendence degree two can be generated by two elements came up in the course of the Niven Lecture delivered by M. Artin at the University of Oregon in the Spring of 1997. The present paper resulted from an attempt to answer this question in the setting of finite-dimensional algebras. The author thanks M. Artin and N. Vonessen for helpful discussions.

REFERENCES

[C] P. M. Cohn, "Algebra," 2nd ed., Vol. 2, Wiley, Chichester, 1982.
[L] S. Lang, "Algebra," Addison–Wesley, Reading, MA, 1965.
[P_1] C. Procesi, Non-commutative affine rings, *Atti Accad. Naz. Lincei (8)* **8**, No. 6 (1967), 239–255.
[P_2] C. Procesi, "Rings with Polynomial Identities," Dekker, New York, 1973.
[Re] Z. Reichstein, On automorphisms of matrix invariants, *Trans. Amer. Math. Soc.* **340**, No. 1 (1993), 353–371.
[RV] Z. Reichstein and N. Vonessen, An embedding property of universal division algebras, *J. Algebra* **177** (1995), 451–462.
[Ro] L. H. Rowen, "Ring Theory," Vol. 2, Academic Press, San Diego, 1988.